Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at http://about.jstor.org/participate-jstor/individuals/early-journal-content.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact support@jstor.org.

THE MODULAR THEORY OF POLYADIC NUMBERS.

By Albert A. Bennett.

1. Introduction. While the study of numbers usually involves the frequent representation of integers in one or another notational system, it is not ordinarily the properties of the method of representation that are studied but rather the intrinsic features of the numbers themselves. It is nevertheless true for example that the time spent in teaching elementary arithmetic for commercial purposes involves not a few hours devoted to the mere technique of manipulating Arabic decimal symbols. The distinction drawn in elementary text books between decimals and fractions is based on the existence of two methods of representing rational numbers and of two partially distinguishable types of problems, each being dealt with more easily in one notation than in the other. Were the classical Roman notation the only one employed, several chapters in the grade school text books on arithmetic would be appearing in very different form. It will be instructive to keep this fact in mind in reading this article, for this discussion will involve properties of numbers in part dependent on a representation similar to the decimal or, more properly speaking, decadic notation. On this account a few words will first be said concerning the decadic notation.

A number in the decadic notation, using Arabic symbols for the digits, is denoted by a sequence of digits, the sequence being not necessarily terminating. A non-integral rational number usually requires a decimal point in its decadic representation. Thus $\frac{1}{2} = .5$, $1/100 = .01$, $\frac{1}{3} = .333 \cdots$, while an integer does not require a decimal point, the figures to the right of the decimal point when written being all zeros. Numerical symbols employing the decimal point fall into two logical classes. In one class the decimal "terminates," that is, after a finite number of digits, the figures form an unbroken sequence of zeros, which zeros need not be expressed. In the other the figures do not "terminate" and no matter how far out one proceeds to the right of the decimal point digits other than zero may be found still further out in each of the expressions of the second class. A number is representable as a terminating decimal if, and only if, it is expressible as P/Q where P and Q are relatively prime and where Q is a factor of some power of 10, the base of the decadic notation. On the other hand, every positive number is representable as a non-terminating decimal by using the fact that

$$1. = .9999 \cdots.$$

Thus $1/2 = .49999 \cdots$, $1/100 = .009999 \cdots$.

Despite one's familiarity in elementary instruction with the idea of a non-terminating decimal, it is ordinarily assumed that no representation which is non-terminating to the left is to be employed. This is however a matter rather of custom and convenience than of logical requirement although a consideration of relative magnitude makes it generally desirable. For example, the notation

$$\cdots,333,334. = x$$

can represent but a single number, which may be readily identified in a few simple steps. If the product $3x$ be formed, it is found to be identically of the form, $\cdots,000,002$, so that x represents, if anything, the number $2/3$.

We shall define a *decadic integer* as a decadic symbol whether or not terminating to the left, but not requiring a decimal point. Thus $.6666\cdots$ is not a decadic integer while $\cdots,333,334$ is a decadic integer although both express the fraction $2/3$. It may be readily proved that every positive rational number P/Q when Q is not a factor of any power of the base, 10, may be written as a decadic integer. It is further to be noted that the negative of a decadic integer is also a decadic integer. For example,

$$-1 = \cdots,999,999.$$

Indeed, decadic integers may be added, subtracted or multiplied with decadic integers for results. Thus decadic integers constitute what is called a domain of integrity. Unlike the case of decimals, the representation of a number as a decadic integer, when at all possible, is unique.

2. Polyadic numbers. A generalization from the decadic representation to a *b-adic representation,* where b is an arbitrary integer greater than unity, involves no difficulties. While a number in decadic representation is also capable of representation in a b-adic system, a decadic integer is not necessarily a b-adic integer. For example, the decadic integer $\cdots,333,334$ cannot be a 3-adic integer since the denominator of $2/3$ is not prime to the base 3. A number may be frequently expanded as an integer simultaneously with respect to n distinct bases and so be represented as a b_1-adic, b_2-adic, $\cdots$, b_n-adic integer. If the bases, b_1, b_2, $\cdots$, b_n, be known, any one representation of course determines the number itself and therefore the other representations also.

A set of independent expressions $(a_1, a_2, \cdots, a_n)$, where a_i is a b_i-adic integer, $i = 1, 2, \cdots, n$, may be studied as in the theory of complex numbers where in particular it may happen that the n symbols denote the same abstract number. By the sum of two such symbols $(a_1, a_2, \cdots, a_n)$ and $(a_1', a_2', \cdots, a_n')$ will be meant the symbol $(a_1 + a_1', a_2 + a_2', \cdots, a_n + a_n')$ and by their product will be meant $(a_1 \times a_1', a_2 \times a_2', \cdots, a_n \times a_n')$. Such a symbol may be called a *polyadic number* and in particular where each element is a respective b-adic integer, the polyadic number is called a *polyadic integer*. In the same manner, b-adic integers to a given set of bases, $b_1, b_2, \cdots, b_n$, constitute a domain of integrity.

When b is a composite number equal to, say, $p_1^{m_1}p_2^{m_2}\cdots p_k^{m_k}$, where the p's are distinct primes, the study of the single b-adic numbers is much enriched by considering their polyadic representations with respect to the k bases, $p_1, p_2, \cdots, p_k$. It is to be noticed that any number which is expressible as a b-adic integer will also be integral in this polyadic representation and the converse is also true. The theory of b-adic numbers may therefore be confined in the first instance to cases where b is a prime, the composite cases being included in the theory of polyadic numbers where each base is a prime.

If $\pi_1, \pi_2, \pi_3, \cdots$ be the successive primes $2, 3, 5, \cdots$, as occurring in their order of magnitude, the polyadic numbers with an infinite number of bases, $\pi_1, \pi_2, \pi_3, \cdots$, may be considered. Any other system will be a *section* of the system so obtained, being the result of omitting some of the bases from this system. This "complete" polyadic system of integers consists therefore of numbers which may be represented by an array

$$\begin{array}{l}
\cdots a_{m1} \cdots a_{31}a_{21}a_{11}a_{01} \\
\cdots a_{m2} \cdots a_{32}a_{22}a_{12}a_{02} \\
\cdots a_{m3} \cdots a_{33}a_{23}a_{13}a_{03} \\
\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\
\cdots a_{mn} \cdots a_{3n}a_{2n}a_{1n}a_{0n} \\
\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot
\end{array}$$

where the nth row denotes the π_n-adic number indicated by the notation, $\cdots + a_{mn}\pi_n^m + \cdots + a_{3n}\pi_n^3 + a_{2n}\pi_n^2 + a_{1n}\pi_n + a_{0n}$.

Not only may sections of the array be considered which correspond to the suppression of certain entire rows, but a more general type of section is of interest where left-hand portions of some rows are suppressed. This may be illustrated in the case of a single p-adic number where p is any prime number.

3. Modular b-adic numbers. Let q be a positive integer and b be any base, and consider the section of b-adic numbers including through the coefficients of b^{q-1} only, all consideration of the coefficient of b^q and higher powers being omitted. In other words, consider the modular theory of b-adic integers, modulo b^q. Addition, subtraction and multiplication may be effected by the usual rules so that the modular b-adic numbers (*mod.* b^q) of themselves constitute a domain of integrity. The theory of b-adic numbers to the modulus b^q, where $b = p_1^{m_1}p_2^{m_2}\cdots p_k^{m_k}$, is included in the theory of polyadic numbers, to the bases, $p_1, p_2, \cdots, p_k$, and to the respective moduli, $p_1^{qm_1}, p_2^{qm_2}, \cdots, p_k^{qm_k}$, which is the study of a section of the general double array of coefficients.

More generally, it is always possible to find a single positive integer whose expansion with respect to n distinct prime numbers, $p_1, p_2, \cdots, p_n$ (n, finite), shall coincide with a given section including only these bases taken *modd.* $p_1^{m_1}, p_2^{m_2}, \cdots, p_n^{m_n}$. Two such numbers will differ in fact by an integral multiple of the product, $p_1^{m_1} \times p_2^{m_2} \times \cdots \times p_n^{m_n}$. This situation no longer persists when n is allowed to become infinite. However, the array may still be treated as a "number" in the sense of a complex number or for n infinite it may be thought of as a sort of fictitious limiting number. Similar remarks apply when one of the exponents, m_i, is allowed to increase indefinitely.

4. Division among b-adic numbers. In a b-adic integer, expressed by the symbol, $\cdots a_m \cdots a_3a_2a_1a_0$, or more explicitly in the form, $\cdots + a_mp^m + \cdots + a_3p^3 + a_2p^2 + a_1p + a_0$, the term a_0 is called the *principal* term of the number. A b-adic integer is said to be *singular* or *nonsingular* according as its principal term does or does not vanish. The words "singular" and "nonsingular" are applied directly to b-adic integers only when b is a prime. For composite bases, b, the representation as a polyadic number to bases which are the distinct prime factors of b is chosen. A polyadic number is singular if any one of its principal terms is zero, and it is nonsingular if, and only if, none of its principal terms vanishes.

Division giving a unique quotient is possible by polyadic numbers with prime bases whether or not in a modular domain if and only if these be nonsingular. In the complete domain, that is, where no modular reductions are made, division by a singular number, no row of which is entirely zero, is possible by the introduction of terms to the right of the "decimal" point, that is, by going outside of the integral domain. In particular, nonsingular polyadic numbers have nonsingular reciprocals. The nonsingular numbers do not form, however, a domain of integrity, since the sum of two nonsingular numbers may be singular.

5. Elementary units. The modular theory of polyadic numbers presents little of interest not found in the simple case of a single p-adic number. Some of the few particular points worth mentioning may be given here. An *elementary unit* is defined as a number whose polyadic representation contains the figure one as a principal term in one row, all other figures of this row and of other rows being zero. Let the modular polyadic numbers be taken *modulis* $p_1^{m_1}, p_2^{m_2}, \cdots, p_k^{m_k}$, and let it be desired to identify the elementary unit which has 1 for the principal term of the row for p_i. Such a number, e_i, has the property that $e_i = 0$, *modd.* $p_1^{m_1}, p_2^{m_2}, \cdots, p_{i-1}^{m_{i-1}}, p_{i+1}^{m_{i+1}}, \cdots, p_n^{m_n}$, while $e_i = 1$, *mod.* $p_i^{m_i}$. As is well known Euclid's algorism for the highest common factor may be applied to a pair of relatively prime numbers P and Q, so as to determine two integers M and N of opposite sign such that

$$MP + NQ = 1,$$

where furthermore M is numerically less than Q and N numerically less than P, so that MP is equal to 1 *modulo* Q and is equal to 0 *modulo* P. By taking P as the product, $p_1^{m_1} \times p_2^{m_2} \times \cdots \times p_{i-1}^{m_{i-1}} \times p_{i+1}^{m_{i+1}} \times \cdots \times p_n^{m_n}$, and Q as $p_i^{m_i}$, an $MP = e_i$ is obtained. The successive elementary units $e_1, e_2, \cdots, e_n$ having been determined, we have $e_1 + e_2 + \cdots + e_n = 1$ (*mod.* b), where $b = p_1^{m_1} \times p_2^{m_2} \times \cdots \times p_n^{m_n}$. The theory of numbers to a composite modulus is fairly illustrated in the case of the modulus $12 = 2^2 \times 3$. The twelve numbers of the set may be represented as follows,

$$1 = \begin{pmatrix} 0 & 1 \\ & 1 \end{pmatrix}, \quad 2 = \begin{pmatrix} 1 & 0 \\ & 2 \end{pmatrix}, \quad 3 = \begin{pmatrix} 1 & 1 \\ & 0 \end{pmatrix}, \quad 4 = \begin{pmatrix} 0 & 0 \\ & 1 \end{pmatrix},$$

$$5 = \begin{pmatrix} 0 & 1 \\ & 2 \end{pmatrix}, \quad 6 = \begin{pmatrix} 1 & 0 \\ & 0 \end{pmatrix}, \quad 7 = \begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix}, \quad 8 = \begin{pmatrix} 0 & 0 \\ & 2 \end{pmatrix},$$

$$9 = \begin{pmatrix} 0 & 1 \\ & 0 \end{pmatrix}, \quad 10 = \begin{pmatrix} 1 & 0 \\ & 1 \end{pmatrix}, \quad 11 = \begin{pmatrix} 1 & 1 \\ & 2 \end{pmatrix}, \quad 12 = 0 = \begin{pmatrix} 0 & 0 \\ & 0 \end{pmatrix}.$$

The elementary units are 9, $= \begin{pmatrix} 0 & 1 \\ & 0 \end{pmatrix}$, and 4, $= \begin{pmatrix} 0 & 0 \\ & 1 \end{pmatrix}$. The upper row is always added 2-adically and the lower 3-adically. The singular numbers are 0, 2, 3, 4, 6, 8, 9, 10. The four nonsingular numbers, 1, 5, 7, 11, are each self-reciprocal. The nonsingular numbers always form a group under multiplication so that a multiplication table of the nonsingular numbers is always of interest—it includes, of course, in particular the reciprocal of each nonsingular number in every case. For the case of 12 as above we have as a multiplication table for the nonsingular numbers, the following self-explanatory tabulation

	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

6. Equivalence and singular classes. Two polyadic numbers are said to be *equivalent* if one is obtained from the other by multiplication by a nonsingular number. In particular, all nonsingular numbers in a given system are equivalent. In general, however, not all singular numbers are equivalent. The test for equivalence is obvious in the typical polyadic expansion. Two polyadic expansions are equivalent when corresponding rows have the same number of consecutive zeros counting from the right. Thus in the above

$$\begin{pmatrix}1 & 0\\ & 2\end{pmatrix}, \begin{pmatrix}1 & 0\\ & 1\end{pmatrix}, \text{ are equivalent,}$$

$$\begin{pmatrix}1 & 1\\ & 0\end{pmatrix}, \begin{pmatrix}0 & 1\\ & 0\end{pmatrix}, \text{ are equivalent,}$$

$$\begin{pmatrix}0 & 0\\ & 1\end{pmatrix}, \begin{pmatrix}0 & 0\\ & 2\end{pmatrix}, \text{ are equivalent,}$$

$$\begin{pmatrix}0 & 1\\ & 1\end{pmatrix}, \begin{pmatrix}0 & 1\\ & 2\end{pmatrix}, \begin{pmatrix}1 & 1\\ & 1\end{pmatrix}, \begin{pmatrix}1 & 1\\ & 2\end{pmatrix}, \text{ are equivalent,}$$

$$\begin{pmatrix}0 & 0\\ & 0\end{pmatrix} \text{ is only self-equivalent,}$$

and the five sets above are mutually non-quivalent.

For any singular polyadic number, a, other than zero there is a corresponding *singular class* $SC(a)$ within which division by a is unique; this singular class consists of all numbers of the total class which have at least the initial zeros of a. Thus if in a in the ith row the first j figures counted from the right are zero then each polyadic number in $SC(a)$ will have zeros for the first j figures from the right in the ith row. The analogue of the singular class for a nonsingular number is the complete class. In the example above we have

$$\begin{aligned}
SC\ (0) &= 0,\\
SC\ (2) &= 0,\ 2,\ 4,\ 6,\ 8,\ 10,\\
SC\ (3) &= 0,\ 3,\ 6,\ 9,\\
SC\ (4) &= 0,\ 4,\ 8,\\
SC\ (6) &= 0,\ 6,\\
SC\ (8) &= SC\ (4),\\
SC\ (9) &= SC\ (3),\\
SC\ (10) &= SC\ (2).
\end{aligned}$$

A singular class is always a domain of integrity and is sometimes a field, that is, division within a singular class is sometimes possible by every number other than zero. The numbers common to two singular classes always constitute a singular class. A singular class whose only singular subclasses are itself and zero is called a *primitive singular subclass.* A singular subclass other than 0 is a field if and only if it is primitive. A primitive subclass consists of numbers whose polyadic expansions consist, except for a single common fixed element, wholly of zeros. There are therefore as many primitive singular subclasses as there are rows in the expansion. A primitive singular unit is defined as $p_i^{m_i-1}e_i$ where e_i is the elementary unit for the modulus, $p_i^{m_i}$. A primitive singular unit generates a primitive singular subclass. The primitive singular units for the modulus twelve are

$$\begin{pmatrix} 1 & 0 \\ & 0 \end{pmatrix} = 6 \text{ and} \begin{pmatrix} 0 & 0 \\ & 1 \end{pmatrix} = 4,$$

where 4 is also an elementary unit.

7. Sets of p-adic numbers with a common base. We shall now turn to the case of sets of p-adic numbers proper with a single common base rather than polyadic numbers with several distinct bases.

Let $(a_0, a_1, a_2, \cdots, a_n)$ be a set of $(n+1)$ p-adic integers, with the common base p, a prime. This set will be called *singular* if and only if *each* of the numbers $a_0, a_1, \cdots, a_n$ is singular. A single set will be said to be of *nullity* s, if there is at least one of the numbers in which the coefficient of p^s does not vanish while the coefficients of p^i, $i = 0, 1, 2, \cdots, s-1$, vanish for each of the $n+1$ numbers of the set. A nonsingular set may be called the *point coördinates* of a point in a *p-adic projective system* provided that two sets are regarded as corresponding to the same point if and only if these sets may be obtained one from the other by multiplication by a nonsingular p-adic number as a factor.

Two points are said to be *neighboring* if a singular set other than zero is linearly dependent on the coördinates of the two respective sets of coördinates. Two points are said to be in a *neighborhood of the sth order*, when a singular set of nullity s is linearly dependent upon their coördinates.

A set of points is *linearly dependent* if the null set, zero, may be expressed as a linear combination of them with nonsingular coefficients. The set is *linearly semi-dependent of order s* when a singular set of nullity, s, may be represented as a linear combination of them with nonsingular coefficients but no singular set of nullity greater than s is so expressible. When no singular set is expressible as a linear combination of the given set with nonsingular coefficients—what may be thought of as semi-dependence of order zero—the given system is *linearly independent.* Thus two semi-dependent points are neighboring.

With these concepts and definitions one may study a modular "geometry" with a composite modulus of the form p^m. This is to be distinguished from the Galois field of p^m where the modulus is merely p. The Galois field is obtained by introducing algebraic irrationalities in the field of p itself. The domain here treated, of p^m, is not a field and in consequence does not yield so natural a form of " geometry." In fact, the limiting type of geometry for s kept fast and greater than unity, while p is allowed to increase indefinitely, is not the usual real geometry but a non-Archimedean theory with actual constant " infinitesimals." For composite numbers not merely powers of primes, the geometrical study is better carried out by considering separately the distinct relatively prime factors each of the form p^s.

A discussion of some related ideas will be found in Fraenkel, Teiler der Null und Zerlegung von Ringen, Journ. f. d. r. u. ang. Math. (Crelle), (145) 1915, (139–176). The notion of p-adic integers is due to K. Hensel. References will be found in the above paper.

Baltimore, Md.,
September, 1920.